Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

Testimony of Julie A. Williams
Director, Federal Civilian Practice
Internet Business Solutions Group
Cisco Systems, Inc.

Hearing Before the

House Committee on Government Reform

"Who's Watching the COOP? A Re-Examination of Federal Agencies' Continuity of Operations Plans"

April 28, 2005

Cisco Systems

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

Chairman Davis, Ranking Member Waxman, and other Distinguished Members: Thank you for the opportunity to testify today regarding Cisco's experience with business continuity planning and the importance of telework as a key enabler of our strategy to provide highly available, responsive, robust, and secure business operations.

My name is Julie Williams and I am the Director of the Federal Civilian Agency Practice for Cisco's Internet Business Solutions Group (IBSG). Our mission is to provide global insight, perspective, and experience to senior level executives and government officials in the use of technology to transform the efficiency and effectiveness of their organizations. In some cases, we help organizations redefine their strategies, create new capabilities, or increase capacity to support the increased demands of a digital society. My role affords me the opportunity to collaborate with a global team of in-depth industry experts, to share best practices with government entities both here and abroad, and to assist these entities in developing technology related public policies and implementation plans aimed at creating maximum public value. Our recent endeavor, a book entitled, "Connected Government", is a collection of essays written by leaders of fourteen countries that highlight the key elements of their successful transformations to a more citizen-centered government.

To accomplish our mission, IBSG draws upon a decade of technological innovation and industry best practices that have enabled Cisco to gain U.S. $2.2 billion in efficiencies by using internet capabilities in key aspects of its business in the 2004 fiscal year.

Today I will focus my comments on Cisco's experience with business continuity planning and the important role telework plays in enabling our continuity strategy.

Business Continuity Planning @ Cisco

As a publicly-traded company, Cisco has a corporate responsibility to its shareholders to maximize shareholder value in all areas of the business. Ensuring business continuity is a critical element of that shareholder responsibility, and the company is

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete

responsible for maintaining a continuous operating infrastructure to support its financial systems and controls. To accomplish this, Cisco has established a robust Business Continuity Management (BCM) framework that defines the key elements required to insure uninterrupted access to mission critical corporate data and resources in the event of a natural disaster, homeland security threat, or other significant interruption. Figure 1 depicts our BCM framework at the highest level:

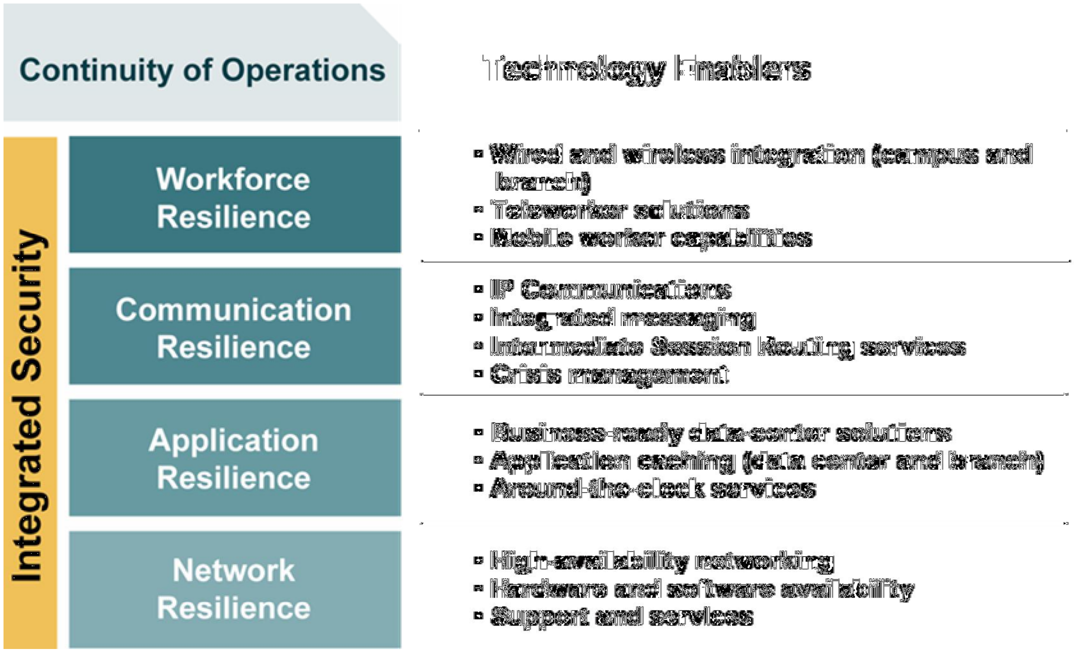

Continuity of Operations
Integrated Security
Workforce Resilience
Communication Resilience
Application Resilience
Network Resilience
Technology Enablers
▪ Wired and wireless integration (campus and branch)
▪ Teleworker solutions
▪ Mobile worker capabilities
▪ IP Communications
▪ Integrated messaging
▪ Intermediate Session Routing services
▪ Crisis management
▪ Business-ready data-center solutions
▪ Application caching (data center and branch)
▪ Around-the-clock services
▪ High-availability networking
▪ Hardware and software availability
▪ Support and services

Figure 1

The framework contains a layered resilience model that integrates all of the traditional business continuity elements into an end-to-end continuity of operations view.   For example, Network Resilience is required to ensure the network is designed for high availability and that the network infrastructure can recover from failure. Application Resilience ensures that critical business applications are not vulnerable to disruption. Communications Resilience provides routing and call management flexibility to maintain communications within and between agencies during disruption, and Workforce Resilience provides capabilities for employees to remain fully connected to enterprise

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete

communications and applications systems even if they cannot report to their normal work location. Each layer of resilience depends on the layers beneath. That is, it is impossible to achieve workforce resilience without a foundation of resilient communications, and it is impossible to provide resilient communications without basing it on a resilient network infrastructure and applications.

Many companies and agencies to date have focused on optimizing the Network, Application, and Communications layers, and largely ignored the Workforce layer in their BCM planning. Cisco has invested heavily in this top layer through focused development of employee tools and teleworking policies. These tools and policies allow us to conduct business anytime, anywhere in the event of significant interruptions and are critical to maintaining shareholder value.

Key Elements

One of our key elements for success is Cisco's corporate Intranet, the Cisco Employee Connection (CEC). CEC provides the foundation for our corporate information and processes worldwide. It gives employees 24 x 7 access to the tools, information, and applications they need to be effective and contribute to our bottom line revenue-generating activities. It was also recently recognized as one of "The Year's Ten Best Intranets: Intranet Design Annual 2005" by the Nielson Norman Group. In effect, CEC becomes just another work "location" such as a cubicle, remote branch office, or public coffeehouse. Today, over 90 percent of Cisco's employees worldwide telecommute for some or all of their workday and many do not have regular physical work locations but work virtually. CEC is their workspace and work "location". This workplace flexibility helps achieve business continuity by dispersing employees on a continuous basis, but it also increases our dependency on thorough end-to-end business continuity management and requires that all of the underlying elements of our BCM framework are solidly in place.

Many of the tools and applications our employees can access via CEC are critical to running the business and delivering against customer commitments. For example, our employees and executives can:

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

- Enter and process customer orders
- Track up-to-the minute performance data including bookings data, revenue, and operating expenses
- Record, distribute and play critical video and audio communications
- Troubleshoot and resolve internal customer issues via our virtual "Network Operations Center – VNOC
- Troubleshoot and resolve external customer issues via our Technical Assistance Center - TAC
- Host / participate in collaborative meetings
- Receive just-in-time training or instructions
- Download software and patches
- Access, manage, and update HR-related information and contacts
- Book business travel and file reimbursement expenses
- Access project and company documentation

Where Does Telework Fit in the COOP Equation?

Teleworking is essential to our continuity of operations plan as it enables access to these critical tools and processes. As stated earlier, many organizations overlook this top element of Workforce Resilience and instead focus on maintaining resilience of core enterprise networks and the resilience of their key enterprise applications. They emphasize connectivity and continuity for the enterprise properties (e.g., branches, headquarters offices) and applications. These are indeed critical assets but are of very little value if the workforce cannot physically enter the enterprise properties. The events of 9/11 and subsequent anthrax threats taught the world that continuity planning must extend beyond the physical buildings and allow workers to connect from anywhere they may be in order to begin planning through and recovering from disruptions.

In order to reliably extend the advanced business applications to the home while incorporating end-to-end security and IT-management polices, Cisco offers the

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete

"Enterprise Business Teleworker" solution to its employees. This solution consists of a small router, an IP-based phone (just like the phone on the employees' office desk), and a PC-mounted video camera. The solution leverages the employee's residential-class cable and DSL broadband access services for connectivity back to the main office or branch location. Key to the success of our telework policy is that Cisco provides 100% reimbursement of the cost of broadband service to employees' homes up to $75 per month. The Federal Government currently reimburses workers up to $100 per month for commuting costs such as Metro, but does not recognize and reimburse the cost of "telecommuting." Only when this policy is changed will the government be able to achieve a robust telework program across all of the agencies.

The router in the home provides advanced end-to-end security features, such as proxy authentication, which establishes the identity of the person logging in. In addition, Network Admission Control establishes the health of the device, before the user is granted access. This helps prevent viruses from propagating through the network. In addition, as legislation to protect personal data is on the rise, all data must be encrypted. The hardware device facilitates this encryption while maintaining network performance for voice and video applications. Cisco's IT organization can both deploy and manage these remote routers directly, without home user intervention, and ensure that corporate security policies are not left in the hands of individuals.

As an example, the major ice storms and snow of 2004 impacted one of our major Research and Development facilities in Raleigh, North Carolina. Our Cisco campus was without electricity for several days, resulting in the complete displacement of more than 2,500 employees until power was restored and roads were safe. Approximately 50 of the North Carolina employees, including several members of the Technical Assistance Center (TAC), were participating in the teleworker pilot program. These employees found that when their homes had power, their teleworker setups were functional, offering them access to the full suite of corporate applications required to maintain business operations.

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

Some employees, when notified that their homes would be without power for an extended period, simply transported their teleworker hardware setup to a location with power and broadband service and continued working. The cost savings were measurable, tangible and substantial. Business continuity was not based on the number of employees who had four- wheel drive, but rather on a secure, managed and fully functional solution.

Measuring the Success of Business Continuity Programs

Business Continuity Management is measured with the objective to identify gaps, test scenarios, and improve responsiveness to disruptions. Our continuity measurements correspond to the four resilience layers and their contribution to continuity. Cisco's measurement approach begins with one fundamental tenant – "Availability should estimate the client experience". This is an important point because measurement can often exist simply to highlight the success of a specific program. However, Cisco's approach is to get as close as possible to measuring the client experience. The implications are surprisingly significant. For instance, one group can measure continuity based on network availability, while the other measures application availability. These two measures will likely yield very different perceptions of availability. It is unlikely that if the network is down, that the client will perceive the application as being up. In fact, their interpretation of the network failure, would likely result in a trouble call that complained that the application was down. Therefore, Cisco's measurements strive to measure complete, end-to-end client experience availability that takes into account application and network performance. A consolidated availability metric is developed from the following:

- Network teams measuring their devices
- Hosting teams measuring their servers
- Webmaster teams testing HTTP against web servers
- Application teams testing synthetic web and database transactions

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

At a business function level, Cisco prioritizes applications and information based on the importance of those applications to the business. Data Centers are allocated to high priority applications and the highest levels of power, security, and availability investment are made to keep those centers in operation. When a metric indicates a compromise of the availability of one of those critical applications, we use the metrics to trigger immediate response from engineering teams to address the problem. Additionally, executive management is given regular briefings on these high priority metrics so the highest level of visibility and attention can be focused on addressing any systematic problems.

These metrics serve as the foundation for supporting the workforce who uses these networks and systems to carry out business. By attending to the Network, Application and Communications layers of resilience in this manner the teleworker, operating in the Workforce resilience layer, is able to be fully productive and engaged even during a disruption.

With this highly available foundation of networks and applications, Cisco employees with virtual offices feel less need to be attached to the Cisco office location and spend more time with customers and partners. Over 90 percent of Cisco's employees' telework one or two days a week. Not surprisingly, the productivity of Cisco teleworking employees has increased as much as 40% since our in-house program began in the late 1990's, and Cisco has realized a 300% return on its investment in secure remote access and mobile workforce programs.

Funding

Shared offices allow Cisco to reduce real estate costs dramatically. Most Cisco sales offices employ shared work space for as many as 6 employees to 1 office space. Employees who need to work in the office simply log into the phone (which establishes their dedicated phone extension number and services to that phone) and turn on their wireless computers to have full office connectivity.

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

In a recent study, Cisco discovered that an advanced shared office space could offer the following cost reductions:

Shared Workspace Cost Savings

Cost Category	**Percent Savings**
Real estate rent: Accommodating more people in the same amount of space	37%
Construction: Building a smaller space than typically required for 140 employees	42%
Workplace services: Reducing utilities and maintenance costs, and nearly eliminating the costs of moves, adds, and changes for workspaces through the use of flexible furniture settings	37%
Furniture: Purchasing less (and slightly less expensive) furniture than typically used in cubicles	50%
IT capital spend: Spending less on switches and switch ports	40%
Cabling: Reducing the number of wired IP cables required per workspace	60%
Equipment room space: Racking fewer switches because of wireless infrastructure	50%

And, the study showed it was accomplished with greater employee satisfaction. This cost, when removed from the on-going budget of an organization, can be used to directly fund other elements of Continuity of Operations.

Security

Cisco's comprehensive security solutions and procedures employed by our IT organization also have prevented Cisco from succumbing to disruption. Internet worms and viruses are a significant threat to continuity because they threaten the performance

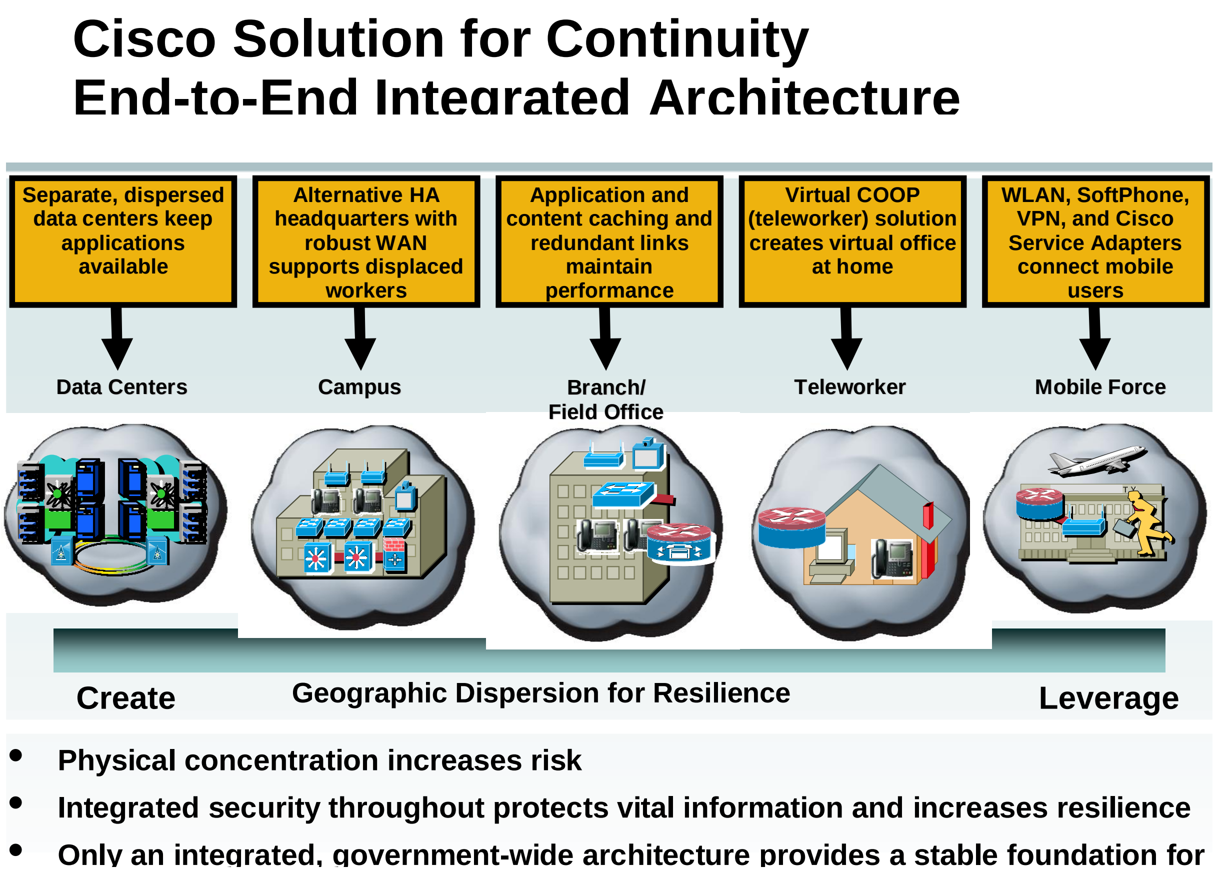
Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

of our network – the nerve center of our business. Because Cisco is heavily dependent on the Internet for employee productivity, sales, partner support, customer support, and manufacturing coordination, we employ our best-in-class products and expertise to monitor and mitigate security threats. In fact, with our security technology and custom tools, we are often able to see a virus or worm threat coming before it hits our network edge. This visibility gives a unique advantage; allowing Cisco to prepare for an attack before it strikes. These advanced security policies, technology, and skills have kept Cisco operating while others of our peers have not.

Incorporating Telework in COOP planning for Industry and Government

Telework is only one of five critical elements that help Cisco achieve a robust continuity of operations capability. As Figure 2 illustrates, the first three – replicating the data center, providing an alternative headquarter location, and ensuring redundant links between branch and field offices – are absolutely essential to support the last two elements of the solution. The teleworking and mobile workforce that will be dispersed in the event of a significant disruption must have access to the mission critical business tools and applications that support the organization’s mission and maintain the public’s trust.

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete



Cisco Solution for Continuity
End-to-End Integrated Architecture

Separate, dispersed data centers keep applications available

Alternative HA headquarters with robust WAN supports displaced workers

Application and content caching and redundant links maintain performance

Virtual COOP (teleworker) solution creates virtual office at home

WLAN, SoftPhone, VPN, and Cisco Service Adapters connect mobile users

- **Physical concentration increases risk**
- **Integrated security throughout protects vital information and increases resilience**
- **Only an integrated, government-wide architecture provides a stable foundation for**

Figure 2

Through our own experience deploying business continuity solutions as well as helping other government and private sector organizations deploying successful programs, we have found several key underlying factors that typically need to be in place to help make the transition an effective and efficient one. They include the following:

- Migrate as much of the organization’s business activities and processes to paperless activities as possible
- Make application tools available to support access and operation in a digital mode
- Ensure full access to all assets from remote locations
- Develop a cultural migration plan for the organization to accept individuals becoming remote individual contributors

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete

- Define and capture new metrics to allow the management process to take place on a virtual basis. For example:
  - Define the nature of tasks for the job and role
  - Define how the effectiveness of an individual contributor can be measured in terms of contributing to the accomplishment of those tasks
  - Define the management support and job support requirements for the individuals working on a virtual basis
- Allow monthly reimbursement of Internet Service Provider (ISP) access for teleworking. Employees should be able to reallocate any unused portions of current transportation commuting costs for this application since it provides similar benefits such as reduced traffic congestion, air pollution, and the like

The success of business continuity planning scenarios and solutions goes beyond the issue of what percent of employees are “eligible” to participate, and instead should focus on including all employees to provide maximum opportunity for a successful continuity of operations plan coverage and deployment.

Continuity of Operations and Telework Solutions for Government

The U.S. Federal Government has established specific Continuity of Operations (COOP) requirements that agencies must meet in order to be able to sustain operations through disruption. Cisco's BCM framework and approach map directly to key technical requirements stipulated in the Federal Preparedness Circular 65 (FPC-65) that each agency must follow.   Figure 3 illustrates the technical requirements in each of the resilience layers of the BCM framework:

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete

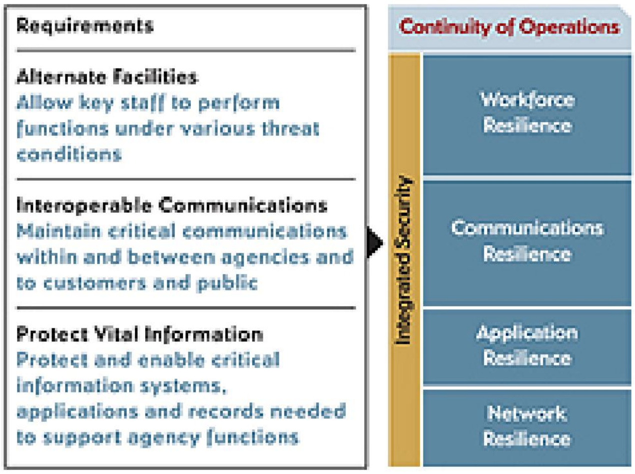

Requirements
Alternate Facilities
Allow key staff to perform functions under various threat conditions
Interoperable Communications
Maintain critical communications within and between agencies and to customers and public
Protect Vital Information
Protect and enable critical information systems, applications and records needed to support agency functions
Continuity of Operations
Integrated Security
Workforce Resilience
Communications Resilience
Application Resilience
Network Resilience

Figure 3

The U.S. Federal Government's COOP requirements for network, application, communications and workforce resilience correspond precisely to the best practices and experiences of the private sector. This is good news, since the private sector can fulfill its obligation to coordinate and support our Government’s continuity through challenges and threats with expertise and technology gained from direct experience. Just as the private sector has discovered, Continuity of Operations and, in particular, Telework is not just a critical asset for sustaining continuity through disruption. It also makes good business sense. It allows agencies to be more efficient, to attract a broader base of skilled employees with flexible work hours and locations, and it provides a far more dynamic and flexible platform for serving government constituents.

A few Federal agencies are in the early stages of establishing teleworking capabilities that easily integrate with their continuity of operations plan. The objective is to provide continuity of operations based on home broadband connectivity or telework versus connectivity from a remote site or alternative disaster recovery site. The reality is that, in the event of a natural disaster or homeland security threat, a large number of government employees will 1) not likely be able to travel to an alternate site due to traffic congestion or 2) not wish to leave their families during the threat. The capabilities include video for real-time command and control decision making from the home office site. It also includes home office use of fuel cell technology which provides an alternative fuel source in the event of a power grid failure. So in the event of a man-

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

made, natural, technological, or national security emergency, the host organization's internal employees will be able to continue essential operations from their home sites or alternate locations securely and under the control of the internal Information Technology department. The main tenets of PDD-67 as well as the Federal Preparedness Circular 65 and EPA Order 2030.1 will have been met. Additionally, avoiding ever having all of the individuals capable of performing a particular function in the same physical location can dramatically reduce terrorist threat vulnerability.

Summary

The U.S. Federal Government has publicly affirmed its responsibility to its citizens by putting into place a plan for sustaining a Constitutional form of Government through any disruption. Continuity of Operations is the means by which the Government plans to fulfill this responsibility, just as Cisco's Business Continuity Management initiative is a means to fulfill our responsibility to our shareholders and employees. We each need the deployment and integration of all four layers in the business continuity model and framework to support the needs of a displaced workforce, and we need to support swift movement toward a true paperless government to help maximize the impact of the tools and processes we employ to manage the nation.

I would like to thank you, Mr. Chairman and other committee members, for inviting me here today. I am happy to answer your questions.